# PROCESSOR AGREEMENT

This **PROCESSOR AGREEMENT** is dated **07/10/2019**

## PARTIES:

(1) Hendy CP School whose address is Iscoed Road Hendy Carmarthenshire SA40XD **(Controller)**

(2) Steps Along the Way Ltd (trading as "Motional") incorporated and registered in England with company number 10980863 whose registered office is at 5F, South Hams Business Park, Kingsbridge, Devon, TQ7 3QH **(Processor)**

## BACKGROUND:

(A) The Controller and the Processor entered into a contract for mental health and wellbeing measurement services on 07/10/2019 (Services Agreement) that may require the Processor to process Personal Data on behalf of the Controller.

(B) This Processor Agreement (Agreement) sets out the terms and conditions on which the Processor will process Personal Data when providing services under the Services Agreement. This Agreement contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation ((EU) 2016/679) for contracts between controllers and processors.

## AGREED TERMS:

### 1. DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation apply in this Agreement.

**1.1 Definitions:**

**Data Protection Legislation:** all applicable data protection laws including GDPR and any applicable national implementing laws, regulations and secondary legislation relating to the processing of Personal Data and the Privacy and Electronic Communications Directive (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426).

**Data Subject:** an individual who is the subject of Personal Data.

**GDPR:** General Data Protection Regulation ((EU) 2016/679).

**Personal Data:** means any information relating to an identified or identifiable natural person that is processed by the Processor as a result of, or in connection with, the provision of the services under the Services Agreement; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Personal Data Breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

**Processing:** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.2 The Schedules form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Schedules.

1.3 A reference to writing or written includes email.

## 2. PROCESSING PURPOSES

2.1 The Controller and the Processor acknowledge that the Controller is the controller and the Processor is the processor and that the Controller retains control of the Personal Data and remains responsible for its compliance obligations under Data Protection Legislation.

2.2. Where the Processor appoints a subcontractor pursuant to clause 4 below, the Processor shall be a data controller in relation to such processing.

2.3 The Processor may process the Personal Data categories and Data Subject types set out in Schedule 1 of this Agreement.

## 3. PROCESSOR'S OBLIGATIONS

3.1 The Processor shall:

3.1.1 implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of Data Protection Legislation and ensure the protection of the rights of the Data Subject, as further set out below in this Agreement;

3.1.2 only use subcontractors to help with the processing of Personal Data in the circumstances set out in clause 4 below;

3.1.3 process the Personal Data only on documented instructions from the Controller or when the Controller or the Controller's authorised agent use our system to initiate the processing, unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

3.1.4 ensure that persons authorised to process the personal data (such as its employees) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

3.1.5 take the security measures set out in clause 5 below;

3.1.6 taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights as set out in clause 6 below;

3.1.7 assist the Controller in ensuring compliance with the obligations set out in clause 7 below (data breach) taking into account the nature of processing and the information available to the Processor;

3.1.8 at the choice of the Controller, delete or return all the Personal Data to the Controller after the termination or expiry of the Services Agreement and delete existing copies (unless Union or Member State law requires storage of the Personal Data);

3.1.9 make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of GDPR and allow for and contribute to audits, including

inspections, conducted by the Controller or another auditor mandated by the Controller;

3.1.10 assist the Controller in ensuring compliance with the requirement to carry out Data Protection Impact Assessments as set out in Article 35 of GDPR, taking into account the nature of processing and the information available to the Processor;

3.1.11 Designate a Data Protection Officer if required by Article 37(1) of GDPR and in accordance with the provisions of Articles 37, 38 and 39 of GDPR; and

3.1.12 immediately inform the Controller, if in the opinion of the Processor, an instruction from the Controller infringes Data Protection Legislation.

3.2 The Processor will promptly comply with any request by or instruction from the Controller to process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3 The Processor will immediately notify the Controller if in its opinion, the Processor carrying out the processing of Personal Data on an instruction from the Controller would infringe any provision of Data Protection Legislation.

3.4 The Processor will keep all Personal Data confidential and not disclose such data to third parties unless specifically authorised in writing by the Controller or as required by law. If the Processor is required by law, court, regulator or supervisory authority to process or disclose any Personal Data, the Processor will first inform the Controller of this and allow the Controller to object or challenge the requirement, unless the law prohibits the Processor from informing the Controller.

## 4 SUBCONTRACTORS

4.1 The Processor may authorise a third party (“subcontractor”) to process the Personal Data if:

4.1.1 the Processor and the subcontractor enter into a written contract containing terms the same as those set out in this Agreement, in particular, in relation to data security measures; and

4.1.2 the Processor maintains control over all Personal Data it shares with the subcontractor; and

4.1.3 the Processor ensures that the subcontractor does not process the Personal Data except on instructions from the Data Controller (unless required to do so by Union or Member State law).

4.2 The Processor shall be responsible for the subcontractor’s performance of obligations.

## 5. SECURITY

5.1 The Processor shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:

5.1.1 the pseudonymisation and encryption of Personal Data;

5.1.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

5.1.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

5.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

5.2 In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

## 6. RESPONSES TO DATA SUBJECTS

6.1 The Processor will put in place such technical and organisational measures as may be appropriate to enable the Controller to comply with the rights of Data Subjects under Data Protection Legislation, including the right of access, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability, the right to object to processing and the right to object to automated individual decision making.

6.2 If the Processor receives any complaint or other communication relating to the processing of the Personal Data or a Subject Access Request from a Data Subject, it must notify the Controller as soon as possible after it receives it and will provide the Controller with all reasonable assistance in helping the Controller to reply to such communications.

6.3 The Processor will provide to the Controller such information as the Controller may reasonably require in order for the Controller to comply with the rights of Data Subjects under Data Protection Legislation.

6.4 The Processor will provide all appropriate assistance to the Controller to enable it to comply with any information or assessment notices served on the Controller by any supervisory authority under the Data Protection Legislation.

6.5 The Processor shall not disclose Personal Data to any third party other than at the Controller's written request or as set out in this agreement or as required by law.

## 7. PERSONAL DATA BREACH

7.1 If any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable ("Personal Data Loss"), the Processor will notify the Controller without undue delay after learning of such Personal Data Loss.

7.2 If the Processor becomes aware of any unauthorised or unlawful processing of the Personal Data or any Personal Data Breach, it will notify the Controller without undue delay including all relevant information such as:

(a) a description of the nature of the Personal Data Breach, the unauthorised or unlawful processing and/or the Personal Data Loss, including the categories and approximate number of both Data Subjects and Personal Data records concerned;

(b) the likely consequences; and

(c) description of the measures taken, or proposed to be taken, including measures to mitigate the impact.

7.3 The parties will co-ordinate and co-operate with each other to investigate any matters arising as contemplated by this clause.

7.4 The Processor agrees that it shall not (and the Controller is solely responsible to):

(a) provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or any other third party, except when the Processor (as opposed to the Controller) is required by law or regulation to provide such notice; and

(b) offer any type of remedy to affected Data Subjects.

## 8. CROSS-BORDER TRANSFERS OF PERSONAL DATA

8.1 The Processor (or any subcontractor of the Processor) shall not transfer or otherwise process Personal Data outside the European Economic Area (EEA) without obtaining the Controller's prior written consent (except where the Processor is required to transfer such data by Union or Member State law, in which case the Processor shall inform the Controller of such legal requirement before processing takes place, unless any law prohibits such disclosure on important grounds of public interest).

8.2 If the Controller consents to the transfer or other processing of the Personal Data outside of the EEA and no appropriate safeguards exist (such as an adequacy decision or the Processor being part of the EU-US Privacy Shield), the Processor and the Controller will each execute the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Schedule to Commission Decision 2010/87/EU ("SCCs").

8.3 if the Processor appoints subcontractors that are based outside of the EEA, the Processor shall, prior to any Personal Data being transferred to such countries, (i) ensure that such subcontractor executes the SCCs and (ii) make available a copy of such executed SCCs to the Controller.

## 9. TERM AND TERMINATION

9.1 This Agreement will continue for so long as the Processor processes any Personal Data related to the Services Agreement (Term).

## 10. DATA RETURN AND DESTRUCTION

10.1 The Processor will, on the request of the Controller, provide the Controller with a copy of or access to the Personal Data in its possession or control in the format and on the media reasonably specified by the Controller.

10.2 On termination or expiry of the Services Agreement, the Processor will retain the Personal Data for a further 6 years.

10.3 If the Controller requires the Processor to delete or destroy certain documents or materials or anything else containing Personal Data, the Processor shall certify in writing that it has so deleted or destroyed the Personal Data within 3 days of doing so.

## 11. RECORDS

11.1 The Processor will keep detailed, accurate and up-to-date records regarding any processing of Personal Data it carries out for the Controller, these are available at any time from the Processor's website – https://motional.io.

11.2 The Controller and the Processor shall review the information listed in the Schedules to this Agreement at least once a year to confirm their current accuracy and update them when required to reflect current practices.

## 12. AUDIT

12.1 The Controller (and any third-party representatives) may audit the Processor's compliance with its obligations under this Agreement and the Processor will give the Controller (and its third-party representatives) all necessary assistance and co-operation to conduct such audits.

## 13. NOTICE

13.1 Any notice or other communication given to a party under or in connection with this Agreement must be in writing and delivered to:

For the Controller: Rhian Kenny at email KennyR5@hwbcymru.net

For the Processor: Lou Gilmour at email lou@motional.io

13.2 Clause 13.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

## 14. GOVERNING LAW

14.1 This agreement, and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims), shall be governed by, and construed in accordance with the law of England and Wales.

14.2 Each party irrevocably agrees that the courts of England and Wales shall have non-exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this agreement or its subject matter or formation (including non-contractual disputes or claims).

This agreement has been entered into on the date stated at the beginning of it.

Signed by Rhian Kenny (Headteacher)

for and on behalf of Hendy CP School

Signed by Neil Gilmour (Director)

for and on behalf of Steps Along The Way Ltd (trading as “Motional”)

# SCHEDULE 1

## PERSONAL DATA PROCESSING PURPOSES AND DETAILS

**Subject matter of processing:** Mental Health and wellbeing assessments and measurements

**Duration of Processing:** while the Controller has an active subscription to Motional

**Nature and Purpose of Processing:** Using our system “Motional” users can upload children’s details, perform assessments, store the results, create programs of activities, and record other details about children.

**Data Subject Types:** Children

**Personal Data Categories:** We process personally identifiable data about children, including information about health, which is a special category.

## APPROVED SUBCONTRACTORS

Some other organisations are indirectly involved in helping us process data. In choosing these organisations, we have ensured that both we and they comply with relevant data protection legislation. There are broadly 4 categories that these subcontractors fall into:

Email Provider
Support System
Website Host
Cloud File Storage

# SCHEDULE 2

## SECURITY MEASURES

Data entered into Motional is encrypted at rest on our servers. We have an SSL certificate to protect data between the user's browser and our server. The server is monitored 24/7 by our hosting company and has robust security in place. This means that if someone broke in to the building and stole the actual server, the information would be incredibly difficult to decrypt. Identifying data is stored separately to results, programs etc., and linked together using our own unique identifier. This means that if even if someone decrypted the data, they could only piece it back together by using our website.

Information sent to us via our support system ("the pink circle") is encrypted. This includes text and files sent.

No hard copies of personal data are produced or stored.

All computers, laptops and devices used by Motional are protected by passwords and firewalls. We don't use public, unsecured wifi networks without taking additional security measures such as VPN connections.

# The Information we used to fill in this agreement

Here are the details you gave us which we used to fill in this Processor Agreement. This page does not form part of the agreement. It is only for your reference.

**Username**
RhianKenny

**User's Email**
KennyR5@hwbcymru.net

**Your Organisation's Legal Name**
Hendy CP School

**Your Organisation's Registered Address**
Iscoed Road Hendy Carmarthenshire SA40XD

**Name of your Data Protection Officer**
Rhian Kenny

**DPO Email Address**
KennyR5@hwbcymru.net

**Who will sign this agreement?**
Rhian Kenny

**Their Job Title**
Headteacher